

UNITED STATES DISTRICT COURT

for the
Southern District of OhioFILED
RICHARD W. NAGEL
CLERK OF COURT

2020 FEB 25 AM 11:39

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)CELLULAR TELEPHONE ASSIGNED
CALL NUMBER 937-381-7919

Case No.

U.S. DISTRICT COURT
SOUTHERN DIST. OHIO
WESTERN DIV. DAYTON
3:20 mj 107

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

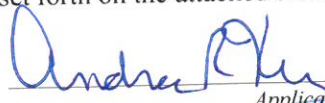
Code Section

See Attachment C

Offense Description

The application is based on these facts:
See Attached Affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Andrea R. Kinzig, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date:

2/25/20

City and state: Dayton, Ohio



Judge's signature

Michael J. Newman, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

Property to Be Searched

1. The cellular telephone assigned call number **937-381-7919** (the “Target Cell Phone”), whose service provider is **Sprint Corporation**, a wireless telephone service provider headquartered at 6480 Sprint Parkway, Overland Park, Kansas, 66251.
2. Information about the location of the Target Cell Phone that is within the possession, custody, or control of Sprint Corporation including information about the location of the cellular telephone if it is subsequently assigned a different call number.

ATTACHMENT B

Particular Things to be Seized

All information about the location of the Target Cell Phone described in Attachment A for a period of thirty days, during all times of day and night. “Information about the location of the Target Cell Phone” includes all available E-911 Phase II data, GPS data, prospective Per Call Measurement Data (PCMD), latitude-longitude data, and other precise location information, as well as all data about which “cell towers” (i.e., antenna towers covering specific geographic areas) and “sectors” (i.e., faces of the towers) received a radio signal from the cellular telephone described in Attachment A.

To the extent that the information described in the previous paragraph (hereinafter, “Location Information”) is within the possession, custody, or control of Sprint Corporation, Sprint Corporation is required to disclose the Location Information to the government. In addition, Sprint Corporation must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with Sprint Corporation’s services, including by initiating a signal to determine the location of the Target Cell Phone on Sprint Corporation’s network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate Sprint Corporation for reasonable expenses incurred in furnishing such facilities or assistance.

This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

ATTACHMENT C

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. §2252(a)(4)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252(a)(2)(B) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §2252A(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. § 2251(a) and (e)	Production of Child Pornography

IN THE UNITED STATES DISTRICT COURT
FOR SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF
THE CELLULAR TELEPHONE
ASSIGNED CALL NUMBER 937-381-7919

Case No. _____

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

INTRODUCTION

1. I make this Affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A) for information about the location of the cellular telephone assigned call number **937-381-7919** (the "**TARGET CELL PHONE**"), whose service provider is Sprint Corporation, a wireless telephone service provider headquartered at 6480 Sprint Parkway, Overland Park, Kansas, 66251. The **TARGET CELL PHONE** is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.
2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A) and coercion and enticement (in violation of 18 U.S.C. §2422). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.
3. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.
4. Based on the facts set forth in this Affidavit, there is probable cause to believe that the following violations have been committed, are being committed, and will be committed by WILLIAM THEODORE HALL, commonly known as "TED" (hereinafter referred to as "HALL"):

- a. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess child pornography;
 - b. 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to distribute and receive child pornography through interstate commerce; and
 - c. 18 U.S.C. § 2251(a) and (e), which make it a crime to produce or attempt to produce child pornography.
5. There is also probable cause to believe that the location information described in Attachment B will constitute evidence of these criminal violations and will lead to the identification of the locations where computer devices are utilized in the commission of the offenses.

PERTINENT FEDERAL CRIMINAL STATUTES

6. 18 U.S.C. § 2251(a) and (e) states that it is a violation for any person to knowingly employ, use, persuade, induce, entice, or coerce any minor to engage in, or to have a minor assist any other person to engage in, or to transport any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, when he knew or had reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or attempts or conspires to do so.
7. 18 U.S.C. § 2252(a)(2)(B) and (b)(1) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

8. 18 U.S.C. § 2252A(a)(2) and (b)(1) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
9. 18 U.S.C. § 2252(a)(4)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
10. 18 U.S.C. § 2252A(a)(5)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

BACKGROUND INFORMATION

Definitions

11. The following definitions apply to this Affidavit and Attachment B to this Affidavit:
 - a. “**Child Pornography**” includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

- b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
- c. **“Minor”** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
- d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).
- e. **“Internet Service Providers”** or **“ISPs”** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.
- f. An **“Internet Protocol address”**, also referred to as an **“IP address”**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

- g. **“Hyperlink”** (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
- h. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- i. **“Uniform Resource Locator”** or **“Universal Resource Locator”** or **“URL”** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.
- j. A **“Smartphone”** is a mobile cellular telephone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded applications.
- k. **Wi-Fi** is a technology that allows electronic devices to connect to a wireless LAN network. Devices that use Wi-Fi technology include personal computers, video game consoles, smartphones, digital cameras, tablets, and modern computers.
- l. The terms **“records,” “documents,”** and **“materials,”** as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Telegram Messenger

12. Telegram Messenger is a cloud-based instant messaging and voice over IP service that was developed by Telegram Messenger LLP, a privately-held company registered in London, United Kingdom. The application can be downloaded and used free of charge on smartphones, tablets, and computers.
13. Telegram Messenger allows users to exchange messages, photographs, videos, and files of any type. Users can also create groups for up to 200,000 people or channels for broadcasting to unlimited audiences. In addition, Telegram allows users to make voice calls to other users.
14. Messages and media in Telegram are client-server encrypted and stored on servers by default. Telegram's special "secret" chats use end-to-end encryption, leaving no trace of the chat's on Telegram's servers. The secret chats provide users the option to self-destruct messages and prohibit users from forwarding the messages. When users set the self-destruct timer on secret messages, the messages will disappear from both the sender's and receiver's devices when the timer expires.
15. Telegram users have the option to create a user name that is displayed to other users. User names are uniquely assigned on a first-come, first-serve basis. Users have the ability to conceal their user names from others so that they can utilize Telegram anonymously.
16. Based on my training and experience, I know that individuals involved in child pornography and child abuse offenses have utilized Telegram Messenger to trade child pornography files and to communicate with other offenders and victims. In my experience, a number of offenders utilize Telegram's security features to avoid detection from law enforcement officers.

Other Social Media Applications

17. Facebook Inc. is a company based in Menlo Park, California. Facebook Inc. owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.
18. Grindr is a geospatial networking and online dating application geared towards gay, bi-sexual, and trans-sexual people. The application runs on iOS and Android mobile

devices. It uses a mobile device's geolocation data to allow users to locate other users who are nearby.

19. WhatsApp is a freeware, cross-platform messaging and Voice over IP (VoIP) service owned by Facebook Inc. It allows users to send text messages and voice messages; make voice and video calls; and share images, documents, user locations, and other media. WhatsApp's client application runs on mobile devices but is also accessible from desktop computers that are connected to the Internet.
20. Based on my training and experience, I know that individuals involved in child pornography and child exploitation offenses have utilized various social media applications, including Grindr, WhatsApp, and Facebook, to trade child pornography files and to communicate with other offenders and victims.

FACTS SUPPORTING PROBABLE CAUSE

21. Beginning in or around December 2019, I have been involved in an investigation of child pornography offenses committed by an adult male who will be referred to for purposes of this Affidavit as "Adult Male A". On or around January 9, 2020, a federal search warrant was executed at Adult Male A's residence in Dayton, Ohio. Various electronic media were seized pursuant to the search warrant, including an Apple iPhone. A subsequent search of the iPhone revealed that Adult Male A had utilized the Telegram and WhatsApp Messenger applications to trade child pornography files with others and to discuss the sexual exploitation of children.
22. During the execution of the search warrant, Adult Male A agreed to be interviewed. I have also conducted several follow-up interviews of Adult Male A in or around January 2020. During these interviews, Adult Male A admitted that he utilized the Telegram Messenger application to trade child pornography files with others. Adult Male A identified that one of these individuals was an adult male who lived in or near Piqua, Ohio. Although Adult Male A could not recall this man's name, Adult Male A identified the man via photograph as HALL. Below is a summary of information that Adult Male A provided about HALL during the various interviews:
 - a. Adult Male A met HALL on the Grindr online dating application approximately one to two years ago, when Adult Male A was living in Piqua, Ohio. Prior to meeting HALL, Adult Male A had not been involved in child pornography offenses. HALL was the first person who sent Adult Male A child pornography files.
 - b. HALL first talked to Adult Male A about child pornography on the Grindr application. HALL then instructed Adult Male A to download the Telegram application, and they then began communicating on Telegram.

- c. HALL sent Adult Male A images and videos depicting child pornography on the Telegram application. The children depicted in the child pornography files ranged from infant and toddler ages to teenagers. Adult Male A estimated that HALL sent Adult Male A these child pornography files on less than twenty-five occasions. HALL also invited Adult Male A into a group chat on Telegram that exchanged numerous child pornography files. New members could only be added into this group if they were invited into the group by another member.
 - i. Based on my training and experience, I know that some group chats on online messenger applications will only accept new members if existing members invite the new members into the group. In my experience, this provides an added security feature to ensure that the new members are not affiliated with law enforcement.
- d. HALL sometimes came over to Adult Male A's residence in Piqua, Ohio so that they could engage in sexually explicit conduct with each other. There were times when HALL watched videos depicting child pornography that he had on his cellular telephone while engaging in the sexual activities with Adult Male A. Adult Male A was able to see these videos and noted that they depicted HALL engaging in sexually explicit conduct with a male child. Conduct that Adult Male A observed in these videos included HALL touching and fondling the child's buttocks and/or genitals, the child touching HALL's buttocks and/or genitals, HALL providing oral sex to the child, and HALL receiving oral sex from the child.
 - i. Based on Adult Male A's descriptions of these videos, I believe that some or all of them depict child pornography. Given that HALL is depicted in the videos, it is reasonable to believe that he produced the videos.
- e. Adult Male A first stated that he had seen at least two videos that depicted HALL engaging in sexually explicit conduct with the male child. Adult Male A later estimated that he had seen at least four of these videos. It appeared to Adult Male A that the boy depicted in the videos was approximately nine to ten years of age. Adult Male A could see HALL's face in the videos and felt confident that HALL was in fact depicted in the videos.
- f. Adult Male A advised that HALL might have called the child depicted in the above described videos his nephew. HALL talked about baby-sitting the child on past occasions.

- g. There was a time when Adult Male A met HALL at a Walmart store in or around Piqua, Ohio. HALL arrived at the store in a black truck. Adult Male A got into HALL's truck and saw that HALL had a small laptop with him. HALL showed Adult Male A child pornography files on this laptop. It appeared to Adult Male A that HALL had hundreds of child pornography files that were saved in a folder on the laptop. Adult Male A did not see any files on the laptop that depicted HALL engaging in sexually explicit conduct with children.
 - h. Adult Male A stopped communicating with HALL approximately one year ago, when Adult Male A moved out of his residence in Piqua, Ohio. Adult Male A has not received child pornography files from HALL since that time. Adult Male A periodically received messages from HALL over the past approximately one year via Grindr and Facebook, but Adult Male A did not respond to the messages. The last message that Adult Male A received was in late January 2020 via Grindr. Adult Male identified that HALL's Grindr profile name at that time was "Nwor".
 - i. Adult Male A showed me HALL's profile picture as well as the message he received from HALL. I noted that the profile picture depicted the face of a white male wearing a hat and sunglasses. It appeared that HALL was the individual depicted in the photograph (although the hat and sunglasses prevented a more definitive identification).
 - i. HALL was previously on the Friends List of Adult Male A's Facebook account. Adult Male A could not recall HALL's Facebook account name.
 - j. Adult Male A provided a description of HALL that is consistent with HALL's physical appearance. Adult Male A was shown a photograph of HALL, and Adult Male A confirmed that the individual depicted in the photograph was HALL.
 - k. Adult Male A never communicated with HALL via telephone, and Adult Male A did not know HALL's telephone number.
 - l. Adult Male A had never been to HALL's residence. Based on HALL's comments, Adult Male A believed that HALL lived in Piqua, Ohio with a relative.
23. On or around November 29, 2019, an adult male who will be referred to for purposes of this Affidavit as "Adult Male B" submitted an online tip to the FBI's National Threat Operations Center (the FBI's telephone and online complaint system). Adult Male B reported that he recently met a man on the Grindr dating application, and that this man talked about molesting his nephew. I later conducted two interviews of Adult Male B in or around December 2019 and January 2020. Adult Male B reported that he knew the

man he met on Grindr as “Teddy” (a common nickname for HALL’s middle name, and similar to HALL’s known alias, as detailed below). Adult Male B also positively identified HALL from a photographic lineup. The information that Adult Male B provided about HALL during the interviews is consistent with the information provided by Adult Male A. At this time, I am not aware of Adult Male A and Adult Male B being acquainted with each other.

24. In summary, Adult Male B provided the following information about HALL in his online complaint and during the two interviews:

- a. Adult Male B met HALL in or around November 2019 on the Grindr dating application. HALL offered to provide drugs to Adult Male B, and they coordinated to meet with each other. HALL picked up Adult Male B in a dark blue truck (similar to the vehicle Adult Male A saw HALL drive to the Walmart store, as detailed above). While they were in a parking lot, HALL and Adult Male A used a quantity of methamphetamine that HALL provided. HALL then drove Adult Male A to HALL’s residence in Piqua, Ohio.
- b. While at the residence, HALL took Adult Male B to a bedroom on the second floor. It was Adult Male B’s understanding that this was HALL’s bedroom. HALL and Adult Male B used an additional quantity of methamphetamine while in the bedroom, which was again provided by HALL.
- c. HALL and Adult Male B engaged in sexual activities with each other in the bedroom. HALL also showed Adult Male B pornographic videos on HALL’s cellular telephone. It appeared that HALL played or streamed these videos from a commercial website. HALL commented that he thought that some of the individuals depicted in the videos were juveniles, as he had seen them on the “dark web”.
- d. HALL made a number of sexually explicit comments about his nephew during the time that Adult Male B was at the residence. Comments that HALL made about his nephew included the following:
 - i. HALL indicated that he had been sexually active with his nephew for around five years. HALL also indicated that he had regular contact with his nephew.
 - ii. HALL made comments indicating he had provided oral sex to the nephew and that the nephew had provided oral sex to him.
 - iii. HALL said that his nephew had masturbated in front of him.

- iv. HALL said that he “collected” things from his nephew.
- v. HALL stated that he had several photographs depicting his nephew nude, but that he would only show Adult Male B one of these photographs.
- e. HALL showed Adult Male B a photograph on HALL’s cellular telephone. This photograph depicted a nude male child kneeling on his knees with his buttocks in the air. HALL said that the boy depicted in the photograph was his nephew. Adult Male B advised that based on the angle that the picture was taken, it was difficult to estimate the age of the boy depicted in the photograph. However, it appeared to Adult Male B that the individual depicted in the photograph could possibly be around sixteen to eighteen years of age.
- f. HALL showed Adult Male B a pair of children’s underwear that was on the dresser in the bedroom. HALL said that this underwear belonged to his nephew. The underwear appeared to be a size for a male child who was approximately six to eight years of age.
- g. Adult Male B questioned HALL about HALL’s possible sexual contact with children. Adult Male B asked if children were sexually different from adults, and HALL responded that they were. HALL commented that children also tasted differently. HALL made comments about wanting to “rape a young straight boy’s ass” (or words to that effect) and to “eat a baby’s ass” (or words to that effect).
- h. As Adult Male B continued to ask HALL questions, HALL seemed to become paranoid. HALL then told Adult Male B to leave the house.
- i. Approximately one month after meeting HALL, Adult Male B and HALL again communicated with each other via Grindr. Adult Male B met HALL again at HALL’s residence. They used methamphetamine together in HALL’s bedroom, but they did not engage in sexual activities with each other or talk about HALL’s nephew.
- j. Around mid-January 2020, Adult Male B sent HALL a message on Grindr asking how HALL was doing. HALL provided a curt response.
- k. HALL and Adult Male B only communicated with each other via Grindr. Adult Male B did not know HALL’s telephone number or Facebook account name.

- l. Based on comments that HALL made, it was Adult Male B's understanding that HALL lived with his father. Adult Male B did not meet or see the father at the residence.
 - m. During an interview on or around January 30, 2020, Adult Male B accessed and showed me HALL's Grindr profile picture.
 - i. I noted that HALL's profile name was "Nwor", and that it contained the same profile name and picture that Adult Male A had showed to me during one of his interviews (which was a few days prior).
 - n. Based on the description that Adult Male B provided of HALL's residence, Adult Male B was shown various photographs of residences that were in this geographic location. Adult Male B identified that photograph depicting 1435 Covington Avenue in Piqua, Ohio (hereinafter referred to as the "SUBJECT PREMISES") was HALL's residence.
 - o. HALL made a comment on one occasion that he was employed as a bartender at the Masque night club in Dayton, Ohio
 - p. Adult Male B was shown a photographic lineup depicting six white males, one of whom was HALL. Adult Male B positively identified HALL from this lineup.
25. Records from the Ohio Bureau of Motor Vehicles identified that HALL utilized the SUBJECT PREMISES when renewing his Ohio driver's license in 2016. His license was suspended in 2017 and has not been reinstated since that time. Records from the Miami County Auditor's Office identified that William M. Hall owns the SUBJECT PREMISES. Based on his name and date of birth, it appears that William M. Hall is HALL's father or other relative.
26. Records from the Montgomery County (Ohio) Jail identified that HALL was arrested in or around July 2016 for a theft offense and in or around March 2017 for a drug offense. The arresting officers for both arrests noted that HALL's address was the SUBJECT PREMISES when booking him into the jail.
27. As part of the investigation, I obtained a report from the Piqua (Ohio) Police Department regarding suspicious activity at the SUBJECT PREMISES on or around August 12, 2019. According to the report, HALL called 911 from the **TARGET CELL PHONE** and reported that someone had stolen the pump from the swimming pool that was on the property. The report identified that HALL used the name "TED" and that his cellular telephone number was 937-418-2403 (hereinafter referred to as "CELL PHONE-2").

- a. It was noted that the telephone number that the officer listed for HALL in the report was different from the telephone number that HALL used to call 911. Based on my training and experience, I know the following:
 - i. When writing reports, law enforcement officers sometimes utilize the last known telephone numbers that are documented in the police department's records system if the officers were not able to obtain the person's telephone number during their contact with those individuals.
 - ii. Some individuals own and utilize multiple cellular telephones.
 - iii. In cases where individuals utilize their cellular telephones to conduct illegal activities, it is not uncommon for them to report false cellular telephone numbers to law enforcement officers.
- 28. Sprint Corporation was identified as the service provider for the **TARGET CELL PHONE**. On or around January 29, 2020, Sprint Corporation was served with a subpoena requesting subscriber information for the **TARGET CELL PHONE**. Records received in response to the subpoena identified that the **TARGET CELL PHONE** was subscribed to William Clemens at an address that is in close proximity to the SUBJECT PREMISES. However, the billing address for the account was the SUBJECT PREMISES. The account was activated on or around September 28, 2019.
 - a. Based on my training and experience, I know that individuals involved in illegal activities often conceal their identities when signing up for various telephone and Internet accounts. It is not uncommon for such individuals to utilize the names and/or addresses of their spouses, girlfriends/boyfriends, family members, or other associates in order to conceal their identities and/or the locations of their residences.
 - b. Also based on my training and experience, I know that some individuals sign up for "family plans" for telephone accounts in order to obtain cost savings. In these cases, the telephone accounts for all individuals on the family plan may be held in one person's name.
 - c. Furthermore, given that HALL utilized the **TARGET CELL PHONE** to call 911 in August 2019 but the Sprint account was not activated until September 2019, it appears that the **TARGET CELL PHONE** was previously serviced by another telephone provider.
- 29. Verizon was identified as the service provider for CELL PHONE-2. On or around January 29, 2020, Verizon was served with a subpoena requesting subscriber information

for CELL PHONE-2. Records received in response to the subpoena identified that the number belonged to a TracFone¹, and that no subscriber information was maintained by Verizon for the account.

30. On or around February 19, 2020, I reviewed publicly available information on the Facebook website for possible accounts utilized by HALL. I located an account with a profile name of "TED HALL" and an account name of **RitABee78**. Although the current profile picture for the account depicted a generic picture, there were numerous former profile pictures and other photographs posted to the account that depicted HALL. Based on this and other information detailed in the Affidavit, I believe that HALL is the user of the **RitABee78** Facebook account.
31. Consistent with the information provided by Adult Male B, the publicly available profile information for the **RitABee78** Facebook account identified that HALL was formerly employed at the Masque night club. Review of historical information on the account's publicly available timeline revealed the following information:
 - a. On or around November 22, 2015, HALL posted a picture to his account that depicted him and a juvenile male child. This child appeared to be approximately four to six years of age and was wearing pajamas. HALL and the child appeared to be in the kitchen of a residence. HALL posted the following caption with the picture: "My nephew [male name]! This boy is growing so fast!!!".
 - b. On or around December 14, 2015, HALL changed the profile picture for his account. The new profile picture depicted HALL and the same juvenile male child from the pictured posted on or around November 22, 2015. The child was wearing what appeared to be the same pajamas from the previous photograph, and HALL and the child appeared to be in the same kitchen.
 - c. Another user utilizing the Facebook display name of "William Clemens" (the name of the subscriber for the **TARGET CELL PHONE**) had posted comments to HALL's Facebook account on at least one occasion.
32. As detailed above, approximately one to two years ago, Adult Male A observed child pornography videos on HALL's cellular telephone that depicted HALL engaging in sexually explicit conduct with a male child who appeared to be approximately nine to ten years old. Adult Male A believed that HALL referred to this child as HALL's nephew, and HALL talked about babysitting the child. Also as detailed above, HALL posted pictures of his purported nephew on his Facebook account in November and December 2015 (a few years prior to the child pornography videos Adult Male A observed on

¹ TracFone Wireless Inc. is an American prepaid, no-contract mobile phone provider. TracFone Wireless operates as a mobile virtual network operator, holding agreements with other wireless network operators (including Verizon, AT&T Mobility, T-Mobile, Sprint Corporation, and U.S. Cellular) to provide service to its customers.

HALL's cellular telephone), and this boy appeared to be approximately four to six years old at that time. Based on this and other information detailed in the Affidavit, it is reasonable to believe that the child depicted on HALL's Facebook account might also be the same child depicted in the child pornography videos that Adult Male A observed on HALL's cellular telephone.

33. On or around February 20, 2020, Facebook Inc. was served with a subpoena requesting subscriber information for the **RitABee78** Facebook account as well as logs of IP addresses utilized to access the account. Review of these records provided the following information:
- a. The account was created on or around January 24, 2009, in the name of "TED HALL". The email address of wtedh78@yahoo.com was the registered email address for the account.
 - b. The following cellular telephone numbers were associated with the **RitABee78** Facebook account: **TARGET CELL PHONE**, CELL PHONE-2, 937-214-0594 (hereinafter referred to as "CELL PHONE-3"), and 937-418-8611 (hereinafter referred to as "CELL PHONE-4"). Facebook Inc.'s records identified that these numbers were "verified" in that the account user had responded to text messages that Facebook Inc. had sent to the user.
 - c. Facebook Inc. provided a log of IP addresses that had been utilized to log into and out of the **RitaBee78** Facebook account during the approximate time period of July 13, 2019 through February 18, 2020. This log identified that from approximately October 17, 2019 through February 18, 2020, the only IP addresses utilized to access the **RitABee78** Facebook account were IP addresses serviced by Sprint Corporation and Charter Communications. The use of IP addresses serviced by Sprint Corporation is consistent with someone using the data plan from his/her cellular telephone to access his/her Facebook account. The use of IP addresses serviced by Charter Communications is consistent with someone using wireless Internet service at a residential or business location to access his/her Facebook account.
 - i. As detailed above, Sprint Corporation is the service provider for the **TARGET CELL PHONE**. The investigation has determined that AT&T is the service provider for CELL PHONE-3, and Verizon is the service provider for CELL PHONE-2 and CELL PHONE-4. Based on the logs of IP addresses provided by Facebook Inc. as well as other information detailed in the Affidavit, it is reasonable to believe that HALL is presently using the **TARGET CELL PHONE** to access his Facebook account as well as other Internet accounts.

- d. The log of IP addresses identified that from approximately July 13, 2019 through September 22, 2019, the only IP addresses utilized to access the **RitABee78** Facebook account were IP addresses serviced by AT&T Mobility and Charter Communications. The use of IP addresses serviced by AT&T Mobility is again consistent with someone using the data plan from his/her cellular telephone to access his/her Facebook account.
 - i. Based on the log of IP addresses provided by Facebook Inc. and other information detailed in the Affidavit, it is reasonable to believe that HALL previously utilized a cellular telephone that was serviced by AT&T and he currently utilizes a cellular telephone serviced by Sprint Corporation. This information is consistent with the records from Sprint Corporation, which identified that the **TARGET CELL PHONE** was activated on Sprint's network on or around September 28, 2019 (as detailed above).
- 34. On or around February 21, 2020, a subpoena was served to AT&T requesting subscriber information for CELL PHONE-3. Records received in response to the subpoena identified that the financial and billing party for the account was William Clemens, and the user name for the account was "God God". The address listed for both William Clemens and "God God" was the SUBJECT PREMISES. The email address listed for both William Clemens and "God God" was wtedh78@yahoo.com. The account was cancelled on or around October 27, 2019 (consistent with the IP logs provided by Facebook Inc.).
- 35. On or around February 21, 2020, a subpoena was served to Verizon for CELL PHONE-2. Records have not been received from Verizon as of this time.
- 36. On or around February 21, 2020, an FBI investigator searched publicly available information on the Telegram application for accounts associated with the **TARGET CELL PHONE**, CELL PHONE-2, CELL PHONE-3, and CELL PHONE-4. The investigator found that there were Telegram accounts associated with the **TARGET CELL PHONE** and CELL PHONE-3. The Telegram account associated with the **TARGET CELL PHONE** had a display name of "TED HALL", and it was presently offline. The Telegram account associated with CELL PHONE-3 had a display name of "Marshall78 HaWl".
 - a. As detailed above, Adult Male A identified that he previously communicated with and received child pornography files from HALL via Telegram.
- 37. Based on all of the information detailed in the Affidavit, I submit that there is probable cause to believe the following:

- a. HALL has engaged in sexually explicit conduct with his nephew and has produced child pornography depicting this conduct. Evidence of this production of child pornography is contained on one or more of HALL's cellular telephones.
- b. HALL has utilized the Telegram application to distribute and receive child pornography files. He has utilized at least two cellular telephone numbers (including the **TARGET CELL PHONE**) to access his Telegram accounts.
- c. HALL has possessed child pornography files on at least two devices – that being his cellular telephone and a laptop computer.
- d. HALL is the user of the “Nwor” Grindr account. HALL has utilized the Grindr dating website to meet at least some of the individuals to whom he has distributed child pornography files and with whom he has discussed the sexual exploitation of children.
- e. HALL is the user of the **RitABee78** Facebook account, and he has utilized this Facebook account to post pictures of his nephew. He has also utilized this Facebook account to contact at least one of the individuals to whom he distributed child pornography files (that being Adult Male A). As detailed above, the Facebook account contains at least two pictures depicting what appears to be HALL's nephew. Based on all of the information detailed in the Affidavit, it is reasonable the **RitABee78** Facebook account contains information about the victims and co-conspirators of HALL's child pornography activities.
- f. HALL presently uses the **TARGET CELL PHONE**. He has utilized the **TARGET CELL PHONE** as recently as on or around February 18, 2020 to access his Facebook account. He has utilized the **TARGET CELL PHONE** as recently as on or around January 30, 2020 to access his Grindr account.
- g. HALL is the user of the wtedh78@yahoo.com email account, and he has utilized this email account to register his Facebook account as well as potentially other social media accounts that contain evidence of his child exploitation activities.

Cellular Telephone Location Information

38. In my training and experience, I have learned that Sprint Corporation is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as “tower/face information” or “cell

tower/sector records.” Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the “sector” (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device (“GPS”) data.


39. Based on my training and experience, I know that Sprint Corporation can collect cell-site data about the **TARGET CELL PHONE**. I also know that Sprint Corporation collects additional data called Per Call Measurement Data (PCMD). PCMD was developed to aid in improving cellular service in a particular area. It can measure the time it takes a signal to leave a cellular handset and then return back to the tower. Furthermore, I know that wireless providers such as Sprint Corporation typically collect and retain cell-site data and PCMD pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.
40. Based on my training and experience, I know that location information from cellular telephones can be materially relevant in investigations involving child exploitation offenses. This information provides evidence of the travels undertaken by the subject when meeting with possible victims. Data regarding the subjects’ whereabouts as obtained from location information can corroborate statements made by the subjects and victims and provide evidence of the locations where the criminal activities took place. Furthermore, data regarding the subjects’ whereabouts as obtained from the location information can lead to the identification of the places where computer devices used in furtherance of the crime may be present.

AUTHORIZATION REQUEST

41. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c).
42. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the **TARGET CELL PHONE** would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the

seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

43. I further request that the Court direct Sprint Corporation to disclose to the government any information described in Attachment B that is within the possession, custody, or control of Sprint Corporation. I also request that the Court direct Sprint Corporation to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with Sprint Corporation's services, including by initiating a signal to determine the location of the **TARGET CELL PHONE** on Sprint Corporation's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate Sprint Corporation for reasonable expenses incurred in furnishing such facilities or assistance.
44. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the **TARGET CELL PHONE** outside of daytime hours.
45. I further request that the Court order that all papers in support of this application, including the Affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.


Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 25th day of February 2020


MICHAEL J. NEWMAN
UNITED STATES MAGISTRATE JUDGE